UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

INFORMATION ASSOCIATED WITH THE YAHOO ACCOUNT OTAKU_SANEL@SBCGLOBAL.NET THAT IS STORED AT PREMISES CONTROLLED BY YAHOO INC.

Case No. 4:23-MJ-6267 PLC

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 U.S.C. § 2251 (sexual exploitation of children) and 18 U.S.C. § 2252A (distribution, receipt, and/or possession of child pornography)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Nicholas W Zotos

Applicant's signature

Nicholas Zotos, Special Agent

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date: 09/22/2023

Patricia L. Cohen

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: Nathan Chapman

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE YAHOO ACCOUNT **OTAKU_SANEL@SBCGLOBAL.NET** THAT IS STORED AT PREMISES CONTROLLED BY YAHOO INC.	No. 4:23-MJ-6267 PLC SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Yahoo Inc ("Yahoo"), an electronic communications service and/or remote computing service provider headquartered at 770 Broadway, 9th Floor, New York, NY 10003-9562. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since November 2017. I am currently assigned to the HSI office in Saint Louis, Missouri and am affiliated with the Missouri Internet Crimes Against Children Task Force. I investigate federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I completed training on these and related topics through the Federal Law Enforcement Training Center (FLETC), the National Criminal Justice Training Center, the National Law Enforcement Training on Child Exploitation, and through various in-service trainings offered through my agency and external partners. That training includes the requirement to observe, review, and classify numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in several forms of electronic media. I am a graduate of the Treasury Computer Forensic Training Program's Basic Computer Evidence Recovery Training and Basic Mobile Device Forensics courses. I hold an A+ certification from the Computing Technology Industry Association. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from personal observations, training and experience, and information obtained from other law enforcement and witnesses. This affidavit is merely intended to show sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (sexual exploitation of children) and 18 U.S.C. § 2252A (distribution, receipt, and/or possession of child pornography), were

committed by Sanel SMAJLOVIC. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and contraband of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

LOCATION TO BE SEARCHED

7. The location to be searched is Yahoo Account: otaku_sanel@sbcglobal.net (hereinafter referred to as "SUBJECT ACCOUNT"), located at a premises owned, maintained, controlled, or operated by Yahoo Inc, a company headquartered at 770 Broadway, 9th Floor, New York, NY 10003-9562.

BACKGROUND CONCERNING EMAIL

8. In my training and experience, I have learned that the Provider provides a variety of on-line services, including electronic mail ("email") access, to the public. The Provider allows subscribers to obtain email accounts at the domain name sbcglobal.net, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications (including retrieved and unretrieved email for the Provider subscribers) and information

concerning subscribers and their use of the Provider services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

a. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

b. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address

information can help to identify which computers or other devices were used to access the email account.

c. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

d. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the

chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

e. In general, an email that is sent to the Provider is stored in the subscriber's "mail box" on the Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for an extended period of time and, in some circumstances, indefinitely.

PROBABLE CAUSE

9. The investigation, described more fully below, involves individuals who have engaged in the sexual exploitation of children through an internet-based, videoconferencing and chat application known as Skype. Based on the investigation, there is probable cause to believe that the user of the SUBJECT ACCOUNT has engaged or attempted to engage in the sexual exploitation of minors in violation of federal criminal statutes, and that evidence of that conduct will be found within the contents of that account.

Background on Online Child Sex Trafficking and Exploitation via Webcam and the Internet

10. HSI is investigating individuals who provide access to pre-produced child sexual abuse material, and live-streaming online webcam shows involving the sexual abuse of children to paying customers worldwide. This growing transnational child-sexual-abuse industry includes child sex traffickers in, among other places, the Philippines, who collect viewership fees from vetted customers scattered throughout the world. Paying customers often request that these child sex traffickers provide pre-recorded depictions of minors engaging in sexually explicit conduct, or sexually abuse minors in real time during private webcam interactions on a variety of streaming video services and applications, including Skype.

11. Based on my training, experience, and information conveyed to me by other law enforcement agents involved in the investigation of live-streaming depictions of child sexual abuse, I know that it is common for such traffickers in the Philippines and elsewhere to be communicating with a large number of individuals who are paying for access to such material. I also know that it is common for the paying customers to be communicating with other traffickers—and sometimes many other traffickers—who are selling access to similar material over the internet. These individuals often use a variety of money service businesses to pay the traffickers or associates of the traffickers for access to this material, including Western Union, WorldRemit, MoneyGram, PayPal, Xoom, and Remitly. In many instances, customers and traffickers must change payment platforms or create multiple accounts on the same platform using slightly changed identifying information to outpace the efforts of payment platforms in detecting suspicious activity and suspending or disabling accounts deemed as engaging in suspicious transactions.

12. I also know that the purchasing individuals often find ways to capture the live-streamed child sexual abuse and exploitation, either by recording the live shows onto their computers or taking still photographs (including "screen captures" or "screen shots") of the abuse, which can also be stored on the individual's computer or an electronic storage device. Such individuals often also save any pre-produced child sexual abuse material the traffickers provide to their computer or an electronic device for later viewing or distribution.

13. In February of 2023, your affiant received reports from HSI Portland. Based on your affiant's review of the reports, I learned the following:

a. HSI identified an individual (hereinafter referred to as the "TRAFFICKER") operating a child-sex-trafficking network from the Philippines. Based on undercover activity and other investigation, HSI learned that the TRAFFICKER did, in fact, have access to minors to sexually abuse on camera and has offered to provide access, through the TRAFFICKER's Skype account, to visual depictions of one or more minors engaging in sexually explicit conduct in exchange for money.

b. On March 25, 2022, the United States District Court of Maine issued federal search warrant (2:22-MJ-50-JAW) for records pertaining to the Skype account used by the TRAFFICKER. In response, Microsoft provided HSI with information associated with that account on May 13, 2022, and provided additional records on June 8, 2022. The information provided by Microsoft revealed incriminating chat content between the TRAFFICKER and Skype account "xflinkx." Subsequent summons to Microsoft revealed Skype account "xflinkx" lists otaku_sanel@sbcglobal.net as the current email address associated with that account. Your affiant personally reviewed the portion of the search

warrant response which included account "xflinkx" and personally reviewed the summons response related to that account.

14. Between March 3, 2023, and September 18, 2023, your affiant obtained and served 25 Department of Homeland Security (DHS) summons requesting information from various electronic service providers, money services businesses, and other entities to ascertain information pertaining to the Skype username "xflinkx," the SUBJECT ACCOUNT, and their user. Based on the responses to DHS summons, your affiant reviewed records from Yahoo, Inc., PayPal Inc., Microsoft, Xoom, Moneygram, WorldRemit Corp, Google, T-Mobile, and Charter Communications.

15. Your affiant reviewed the available IP connection history for the "xflinkx" Skype account provided by Microsoft and found an IP address capture associated with the account's "Last Modified Date and Time" on August 31, 2019. I then queried that IP address with Charter Communications who provided records showing the subscriber using that IP address at the time as Brana Smajlovic with both billing and service address listed as 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129, and with phone number as 314-255-6957.

16. Based on your affiant's review of records from T-Mobile, phone number 314-255-6957 is registered to Sanel SMAJLOVIC with service address as 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129.

17. Based on your affiant's review of records from Yahoo, Inc., I learned that a user created SUBJECT ACCOUNT on October 5, 2006, and provided initials "SS" in the field asking for first and last name.

18. Your affiant reviewed records from PayPal Inc, for all accounts associated with the SUBJECT ACCOUNT and learned there are a total of 10 active or inactive accounts which used

that email address. Seven of those accounts are in the name of Sanel SMAJLOVIC who is 33 years old and resides at 6942 Colonial Woods Dr., Apt 70, Saint Louis County, Missouri. Two other accounts are in the name of Halid Smajlovic, who is 65 years old, and use the same Colonial Woods address on the account. The final account, which is inactive, uses the same Colonial Woods address and is in the name of Brana Smajlovic, who is 58 years old. The Halid or Brana Smajlovic accounts do not have transaction history within the last five years. Seven out of the ten accounts, including the two accounts in the name Halid Smajlovic, list phone number 314-255-6957 subscribed to Sanel SMAJLOVIC. Two more accounts in the name of Sanel SMAJLOVIC do not list phone number at all.

19. On April 12, 2023, your affiant applied for and was granted a search warrant (4:23-MJ-8078 SRW) for records pertaining to Skype account "xflinkx," held by Microsoft Corporation. Microsoft responded to that warrant on July 10, 2023, and your affiant has/continues to review the records. The response from Microsoft included over 58,000 lines of chat between "xflinkx" and 722 unique usernames, between April 20, 2017, and September 14, 2022. Your affiant's review of that material is ongoing but revealed numerous examples of the user of "xflinkx" soliciting or negotiating for, and in many instances seemingly completing, online live video sex shows involving minor females in the Philippines as young as one year old. The chat logs were explicit enough to make clear "xflinkx" was knowingly paying for and directing sex acts be performed on minors in a live international broadcast. In some instances, the traffickers would send photographs as a sample or advertisement of the minor girls available for "xflinkx" to purchase a show with. Some of these sample images themselves displayed minors engaged in sexually explicit conduct. A more detailed sample of these transactions is contained in paragraph 25 below.

20. Contained within the Microsoft warrant return are several instances where the user of "xflinkx" self-identified himself as Sanel SMAJLOVIC in conjunction with providing payment confirmation details to the traffickers in the Philippines. To be sure, your affiant was able to cross-referenced the date, time, payment amount, and recipient information discussed in the sex trafficking chats with financial transactions from Money Service Business accounts directly linked to Sanel SMAJLOVIC and listing his home address as 6942 Colonial Woods Dr Apt 70, Saint Louis, MO.

21. In other conversations, the user of "xflinkx" identified himself as Sanel in a more social context and refenced employment for the Federal Reserve Bank. Your affiant consulted with the Federal Reserve Board Office of Inspector General (OIG) and confirmed Sanel SMAJLOVIC is employed by the Federal Reserve Bank of Saint Louis and has been so employed since October 30, 2017. Your affiant viewed a public LinkedIn profile for "Sanel S.", which lists his employment as a Senior Software Engineer for the Federal Reserve Bank of Saint Louis. The OIG also provided your affiant with information from Sanel SMAJLOVIC's personnel file which listed a home address of record, as 6942 Colonial Woods Dr., Apt. 70, St. Louis, MO 63129 and personal contact email address as sanelss@gmail.com.

The SUBJECT ACCOUNT

22. In addition to being the primary email address associated with the Skype account "xflinkx," your affiant's review of financial transaction records provided under summons found SUBJECT ACCOUNT is associated with at least eight money service business or payment platform accounts with PayPal and Xoom (A Paypal Inc. Service) that are in the name of Sanel SMAJLOVIC.

23. As an example, your affiant found, SUBJECT ACCOUNT is an additional email address listed for PayPal account 1519143165246381427 which is attributed to Sanel SMAJLOVIC. The account was opened March 3, 2018, and shows open status. The account also lists the phone number subscribed to Sanel SMAJLOIVC and home address of 6942 Colonial Woods Dr Apt 70, Saint Louis, MO 63129. This PayPal account has four attempted payments to a recipient in the Philippines using PinoyLoads.com. According to their website, "PinoyLoads is known as a swift online loading station, where you can load online and send load to the Philippines with confidence." At least one attempted payment through PinoyLoads using this PayPal account corresponds to the date and time that Skype user "xflinkx" negotiated for live sex show involving a five-year-old girl. In the chat, the trafficker and "xflinkx" discuss various ways to make payment. The user of "xflinkx" acknowledged he is banned from multiple payment platforms. Eventually, "xflinkx" acknowledges that payment through "PinoyLoads" worked, but processing the payment may take extra time as a first-time buyer through the platform.

24. In my training and experience, Sanel SMAJLOVIC's use of multiple accounts on the same payment platform, use of multiple different payment platforms, admission that he is banned from several payment platforms, and use of multiple different email addresses in connection with payment platforms is consistent with the behavior of other known examples of traffickers and customers engaged in international trade of live sex shows or child pornography. Moreover, review of email records known to be linked to this illicit activity is likely to reveal associations with other yet to be identified accounts used for online payment, cloud storage, or online chat and live video.

25. On September 13, 2023, a Grand Jury for the Eastern District of Missouri returned a sealed indictment charging SMAJLOVIC with four counts of attempted production of child

pornography. (4:23-CR-00490-SRC-RHH). These four counts relate to the investigation outlined above. A sampling of SMAJLOVIC's chat records for each count is as follows:

a. For Count I, the SMAJLOVIC corresponded with a user (hereinafter, "TRAFFICKER 2") over Skype on February 9, 2019. SMAJLOVIC is told that TRAFFICKER 2 is offering a five-year-old child and 10-year-old child, and a price is eventually negotiated. During the live stream, the SMAJLOVIC makes the following requests/statements to TRAFFICKER 2; "yes do fingering," "put finger in straight I can't see like that," "I want see it go inside hehe," and "show me both girls open pussy." The live stream ends, and TRAFFICKER 2 confirms that he/she has received the SMAJLOVIC's payment.

b. For Count II, the SMAJLOVIC corresponded with TRAFFICKER 2 on August 17, 2019. SMAJLOVIC is told that TRAFFICKER 2 is offering an 11-year-old child, and a price is eventually negotiated. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 2; "ye shes nice cute girl but I like 3-5 more ehe(sic). Even 1-3 sometimes haha," "how deep u can put finger her?", "finger all inside?", "ok hun this time I do for that girl but try find me younger hehe. Or some girl before but more deep? Hehe." When TRAFFICKER 2 tells SMAJLOVIC, "its deep now she getting hurt now," SMAJLOVIC responds, "more deep hun." The live stream ends, and TRAFFICKER 2 confirms that he/she received SMAJLOVIC's payment.

c. For Count III, SMAJLOVIC corresponded with a different user (hereinafter, "TRAFFICKER 3") on October 6, 2018. SMAJLOVIC is told that TRAFFICKER 3 is offering a one-year-old child. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 3; "and lol what u can do with

the 1? Nothing? I think too young for me but can I see? Hehe," "can you open lips more? Hehe," "finger her? Or no?", and "nice hehe." SMAJLOVIC eventually provides TRAFFICKER 3 with payment on October 16, 2018.

d. For Count IV, SMAJLOVIC corresponded with TRAFFICKER 3 on June 23, 2018. SMAJLOVIC is told that TRAFFICKER 3 is offering a six-year-old child and ten-year-old child, and a price is negotiated. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 3; "can u wake the 6?", "I like her more," "ye…wake her for show? Or let her sleep u can still show her hehe," and "tell the 10 to put finger in the 6yo pussy hehe." The live stream ends, and TRAFFICKER 3 confirms that he/she has received the SMAJLOVIC's payment.

26. Your affiant's review of the chat logs pertaining to Skype account "xflinkx" revealed this type of activity occurred until at least August 31, 2019. Your affiant's diligent search of available law enforcement databases revealed no intervening law enforcement action that would have stopped SMAJLOVIC from continuing this conduct. In my experience with similar investigations and in consultation with other law enforcement investigating child sex traffickers in the Philippines, it is common for traffickers and customers to change out account usage on various chat applications, including Skype. In fact, in the chat logs from Microsoft I found examples where the user of "xflinkx" references knowing traffickers from their other username or ID or from other chat rooms or platforms.

27. Therefore, Yahoo's servers are likely to contain stored electronic communications and information concerning the user of SUBJECT ACCOUNT and their use of Yahoo's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Yahoo. Because the warrant will be served on Yahoo, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

31. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

NICHOLAS ZOTOS
Special Agent
Homeland Security Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 22nd day of September 2023.

Patricia L. Cohen
HONORABLE PATRICIA L. COHEN
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with otaku_sanel@sbcglobal.net ("the Account") that is stored at premises owned, maintained, controlled, or operated by Yahoo Inc a company headquartered at 770 Broadway, 9th Floor, New York, NY 10003-9562.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Yahoo Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from June 1, 2008, to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 2251, 2252A(a)(2), and (a)(5)(B), those violations involving Sanel SMAJLOVIC and occurring from at least as early as March 2, 2018, to Present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The production, purchase, receipt, or possession of child pornography or attempts to commit, including any such contraband material stored within cloud storage or as attachments to messages, even when deleted or marked for deletion;

b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the Account about matters relating to receipt and distribution of child pornography, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by _____, and my official title is _____. I am a custodian of records for_____. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of _____, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of _____; and

c. such records were made by _____ as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature